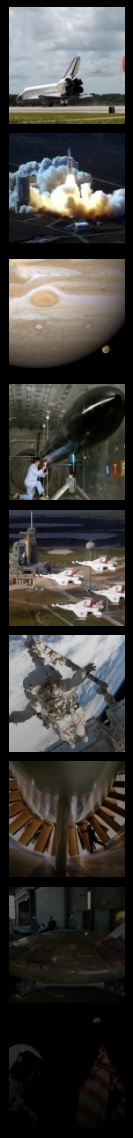
National Aeronautics and Space Administration



What Role Does NASA Leadership Play in NASA Safety?

Watching for Signals, Keeping the Hunger, Setting the Tone

Senior Management ViTS Meeting

May 4, 2015

Hal Bell

Deputy Chief, Office of Safety and Mission Assurance

Winslow Homer. *Eight Bells*, 1886.

This and previous presentations are archived at
sma.nasa.gov/safety-messages

The Problem

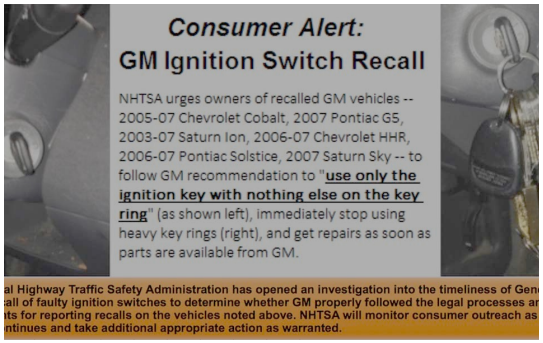
How can we identify a slow drift into a cultural norm that could unknowingly/unintentionally compromise safety?

- A weak signal appears, but by itself is not realized as a cause for concern. Weak (as well as strong) signals of drift should be seen by leaders who know what to look for across a broad vantage by those **who actively seek signals.**
- Are there examples where such signals have been missed?

Winslow Homer. *Eight Bells*, 1886. Source: Addison Gallery of American Art

General Motors Ignition Switch Failures

Feb. 7, 2014: GM recalled 2.6 million cars after linking 13 deaths and 31 crashes to faulty switch design.



GM Consumer Recall. Source: NHTSA

- GM held meetings about the problem as early as 2005; **no action to understand the ignition failures emerged**. At the root of the problem — an engineering design process **without checks and balances.**
  - The ignition switch design engineer had independently changed the part to a more cost-effective design.
  - Chose not to change the part number — masking the hazard source for years. A tone of efficiency within GM's culture led to the ability to both change and approve a part design by a single individual.
- June 5, 2014: Independent investigation by former U.S. Attorney Anton Valukas found that GM's failure to fix the switch design was not due to a cover-up, but rather "their failure to understand, quite simply, how the car was built…although everyone had responsibility to fix the problem, nobody took responsibility."
- A number of GM employees reported they did not take notes at all at critical safety meetings because they believed GM lawyers did not want notes taken. Key gestures indicated a fear of reprisal and litigation.
  - GM Salute: arms crossed, finger pointed at others
  - GM Nod: empty gesture of acknowledgment
- "The Cobalt ignition switch passed through an astonishing number of committees… But determining the identity of any actual decision-maker was impenetrable."

Bhopal

Dec. 2, 1984: A Union Carbide plant in Bhopal, India, leaked 27 tons of deadly methyl isocyanate (MIC) gas which spread throughout the city. Of the approximately 500,000 people exposed, about 8,000 died the first week and 20,000 have died to date. More than 120,000 still suffer from ailments linked to the disaster.

- Management allowed for potentially dangerous working environments.
  - Utilizing undersized safety devices
  - Filling of the MIC tanks beyond recommended capacity
  - Reliance on manual operations
  - Lack of skilled operators
  - Inadequate emergency action plans
  - Poor maintenance after the plant ceased MIC production at the end of 1984
- **Several** safety systems were left inoperable due to poor maintenance and others were switched off to **save cost** — including a tank refrigeration system which could have greatly mitigated the extent of the disaster.

Aerospace Engineering Associates Research

Career NASA engineers Larry Ross and Joe Nieberding analyzed 42 aerospace mishaps over five decades.

- Only one of the 42 cases analyzed (Atlas Centaur 24) experienced what was likely a random part failure as the cause of mission loss.
- The other 41 were associated with some form of human error: **management weaknesses**, systems engineering shortcomings, testing deficiencies, missed advance warnings, etc.

Larry and Joe's repeat factors

- Imperfect management
- Normalizing deviations
- Diminished alertness for warning signs
- Team complacency
- Missing design or procedural errors
- Weak testing practices
- Systems engineering shortcomings
- Flawed understanding of how software fails
- Loss of process discipline
- Improper use of "heritage" systems
- Information flow breakdowns

Titan rocket explodes shortly after liftoff. Source: USAF

ASAP is watching…

NASA has communicated decreasing Loss of Crew/Loss of Mission (LOC/LOM) risk thresholds incrementally over the last decade.

- After the 2005 Exploration Systems Architecture Study (ESAS), LOC/LOM acceptable risk was noted by the ASAP as **1/1000** per NASA briefings.
- In 2012, ASAP noted that there was a notional concept for a LOC of **1/700**, which may or may not be close to the final number.
- In 2014, NASA communicated an Exploration Systems Development Technical Performance Measure (ESD TPM) of **1/400** risk for ascent and **1/650** for descent but TBD for In-Space.
- "[The ASAP] emphasized the need for a firm LOC number. The reason this is important is that LOC is the safety performance standard to which the vehicle is designed. If the Program waits until the vehicle is designed to establish that, it does very little good — it doesn't guide design; it serves only to assess design." —2013 ASAP Quarterly Meeting
- **If the actual intent of design requirements incrementally acknowledges higher risk, is this normalization of deviance, or needful, risk-informed decision-making?**

Leaders are watching…

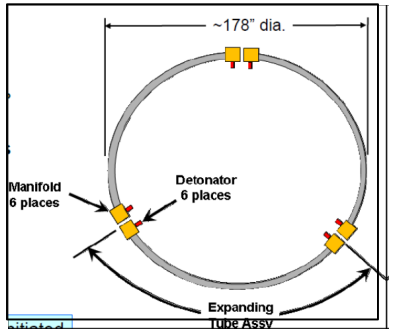
A senior leader alerted OCE and OSMA to four flight hardware test incidents.

- All involved minor electrical/electronic damage; three had been logged in NMIS as close calls.
- Three different projects were involved.
- The incidents took place across a nine-month period.
- All appeared to involve incorrect hardware/test configurations.
- All are still under investigation, but the leader's management team brought their concerns up the chain informally and recommended the alert.
- **This is "walking the talk" to sustain a culture of vigilance — fearless communication by a directorate to cross-check weak signals for underlying common hazards**.

Are we seeing signals today?

- Cost over Mission Suitability and Past Performance becomes a norm rather than an exception.
- Incrementally shaving supposedly minor test elements to align with test affordability rather than ensuring basic test objectives are understood and preserved.
- Not enough funds to investigate when things go wrong.
- Allowing well understood and accepted human rating requirements to transform from timely delivery aligned with ability to influence good design practices to a list of requirements without sensitivity to schedule.
- Serious discussions on getting ourselves comfortable with accepting zero fault tolerant design features in Human Space Flight that, if failure is realized, will result in loss mission and/or crew.
- Investigation findings such as “improper procedures” or “repeat quality assurance shortfalls” or “improper/outdated training”

Apollo Launch Escape System.
Source: NASA



Leadership's Role

Are we watching for and addressing the weak signals?

When risks are identified and elevated, do you have all of the relevant information to make an informed decision?

Is our culture resulting in well-meaning people "accepting" risk without either the authority to do so, or the capability to mitigate that risk to the lowest level necessary?

Let's make sure that we have the hunger — constantly looking for weak signals.

Let's make sure we reflect a culture that does not encourage our workforce to head in the wrong direction — a culture that could ultimately lead to another major catastrophe.

And if you identify that culture, have the courage to intervene.

Thank You